

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
30 mai 2002 (30.05.2002)

PCT

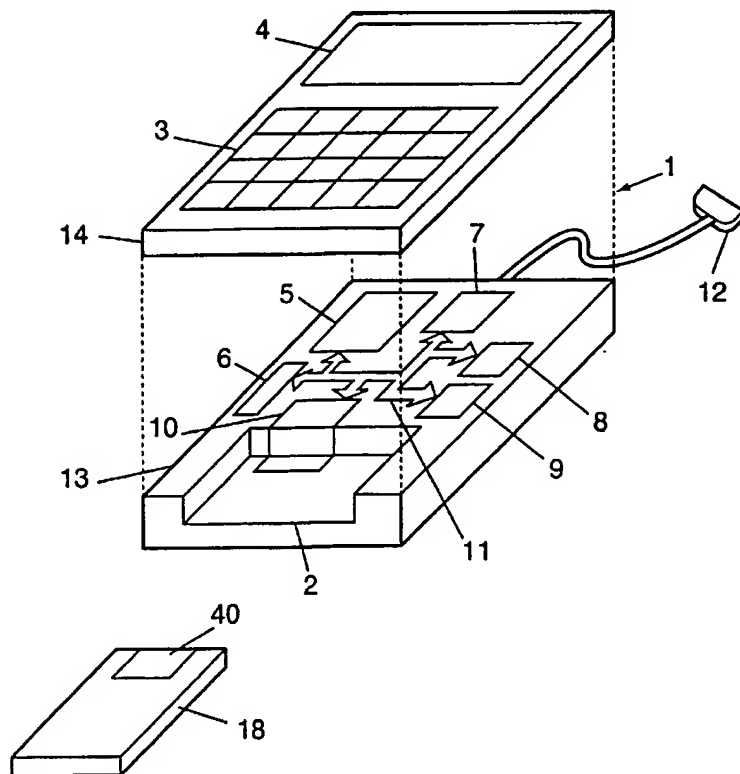
(10) Numéro de publication internationale
WO 02/43016 A1

- (51) Classification internationale des brevets⁷ : G07F 7/10 (71) Déposant (pour tous les États désignés sauf US) : CYBER-
COMM [FR/FR]; 29, rue de Berri, F-75008 Paris (FR).
- (21) Numéro de la demande internationale : PCT/FR01/03569 (72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : MEGGLE,
Claude [FR/FR]; 104, boulevard Arago, F-75014 Paris
(FR).
- (22) Date de dépôt international : 14 novembre 2001 (14.11.2001)
- (25) Langue de dépôt : français (74) Mandataires : DIOU, Jean-Marc etc.; Cabinet Plasser-
aud, 84, rue d'Amsterdam, F-75440 Paris Cedex 09 (FR).
- (26) Langue de publication : français (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
- (30) Données relatives à la priorité : 00/15007 21 novembre 2000 (21.11.2000) FR

[Suite sur la page suivante]

(54) Title: AUTHENTICATING METHOD AND DEVICE

(54) Titre : PROCEDE ET DISPOSITIF D'AUTHENTIFICATION



(57) Abstract: The invention concerns an authenticating device comprising an apparatus (1) for carrying out transactions. The apparatus (1) comprises a housing protected against breaches. In the housing are integrated an interface circuit (10) for receiving an identification support including an identification logic circuit, man-machine interface means (3, 4) for displaying transaction data and for receiving from the user identification data transmitted to the logic circuit via the interface circuit (10) and signature commands related to the transaction data displayed, a protected circuit (6) for delivering a first signature of transaction data in response to signature commands when the identification has been completed, said signature being obtained by encrypting part at least of the transaction data using a non-erasable private signature key stored in the protected circuit.

[Suite sur la page suivante]



WO 02/43016 A1



LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Déclaration en vertu de la règle 4.17 :

- relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement

(57) **Abrégé :** Le dispositif d'authentification comprend un appareil (1) pour effectuer des transactions. L'appareil (1) comprend un boîtier ayant une protection contre les effractions. Au boîtier sont intégrés un circuit d'interface 10 pour recevoir un support d'identification comportant un circuit logique d'identification, des moyens d'interface homme-machine (3, 4) pour présenter des données transactionnelles à un utilisateur et recueillir de l'utilisateur des données d'identification transmises au circuit logique du support via le circuit d'interface (10) ainsi que des commandes de signature en relation avec les données transactionnelles présentées un circuit protégé (6) pour délivrer une première signature des données transactionnelles présentées en réponse aux commandes de signature lorsque l'identification a été effectuée, ladite signature étant obtenue en chiffrant une partie au moins des données transactionnelles au moyen d'une clé privée de signature stockée de façon non effaçable dans le circuit protégé.

PROCEDE ET DISPOSITIF D'AUTHENTIFICATION

Le domaine de l'invention est celui de l'authentification de documents
5 électroniques au moyen d'une signature numérique.

On entend ici par document électronique une suite de nombres sous
forme binaire qui code des données informatiques.

La matérialisation de documents sous forme électronique présente de
nombreux avantages, facilité de stockage, de duplication, de modification, de
10 transmission. Cependant pour certains usages, ces avantages se transforment
en inconvénients.

Par exemple dans le cadre du commerce électronique au moyen de
systèmes ouverts, la transmission de données relatives à une référence de
compte et à un montant à débiter est facilitée par des réseaux ouverts tels
15 qu'Internet. Ces données sont facilement interprétables dans un dialogue entre
système ouvert émetteur et système ouvert récepteur. Cependant, sans
précaution particulière, la duplication, la modification, la transmission de ces
données sont aussi faciles pour un système interceptant les messages que
pour les systèmes émetteurs et récepteurs authentiques.

20 De façon connue, la cryptographie permet de chiffrer le contenu d'un
document de sorte que seul le système récepteur authentique puisse
interpréter le contenu du document.

On distingue la cryptographie symétrique, où une même clé secrète sert
à chiffrer et déchiffrer le document, et la cryptographie asymétrique, où un
25 couple de clés distinctes, l'une privée l'autre publique, est utilisé.

La cryptographie symétrique est adaptée pour un dialogue au sein d'un
couple émetteur récepteur unique avec confiance réciproque car l'émetteur et
le récepteur partagent secrètement la même clé.

La cryptographie asymétrique est mieux adaptée pour établir un
30 dialogue avec de nombreux intervenants potentiels. C'est le cas dans le
commerce électronique où tout acheteur doit pouvoir se mettre en relation
privée avec tout vendeur et tout établissement financier.

Lorsque la clé privée est détenue par le système récepteur, tout système
émetteur peut chiffrer un document au moyen de la clé publique et le
35 transmettre au système récepteur. Seul le système récepteur peut déchiffrer le

document au moyen de la clé privée. Ceci assure la confidentialité du document transmis.

Lorsque la clé privée est détenue par le système émetteur, il est le seul à pouvoir chiffrer le document. Tout système récepteur peut déchiffrer le document, ceci avec l'assurance que le système émetteur qui a transmis le document, est celui qui possède la clé privée.

La mise en œuvre de la cryptographie asymétrique se révèle plus lente que celle de la cryptographie symétrique étant donné que les algorithmes mis en jeu requièrent davantage de calculs. Pour satisfaire des objectifs de rapidité de traitement il convient d'appliquer le chiffrement au moyen d'une clé privée, à des documents de taille faible. Ce mode de chiffrement est bien adapté pour authentifier un émetteur et pour authentifier la véracité d'un document.

Par exemple, pour authentifier un émetteur, le récepteur envoie un document constitué d'une séquence aléatoire à l'émetteur. L'émetteur chiffre le document reçu au moyen de sa clé privée et transmet le document chiffré au récepteur. Le récepteur déchiffre le document chiffré au moyen de la clé publique qu'il sait être celle de l'émetteur. En comparant le résultat à la séquence aléatoire initialement transmise, le récepteur est assuré que l'émetteur est bien celui prévu si le résultat est identique à la séquence aléatoire initialement transmise car l'émetteur prévu est le seul à pouvoir chiffrer le document au moyen de sa clé privée.

Pour authentifier un document original, l'émetteur applique une fonction déterminée au document de façon à obtenir un document qui est généralement de taille réduite. La fonction déterminée peut notamment être une fonction de hachage à sens unique. L'émetteur chiffre le document de taille réduite au moyen de sa clé privée et transmet le document de taille réduite ainsi chiffré au récepteur, accompagné du document original en clair. Le récepteur applique la fonction de hachage à sens unique au document original reçu et déchiffre le document de taille réduite chiffré reçu, au moyen de la clé publique qu'il sait être celle de l'émetteur. Si le résultat de la fonction de hachage est identique à celui du déchiffrement, le récepteur est assuré que le document reçu en clair est identique au document original de l'émetteur.

Un document de taille réduite chiffré au moyen de la clé privée de l'émetteur tel que celui décrit au paragraphe précédent est encore appelé signature électronique du document original. La clé privée est alors souvent appelée clé de signature pour la distinguer d'une clé privée de déchiffrement.

- 5 Un choix de clés privées différentes pour le déchiffrement et pour la signature, permet d'éviter certaines attaques connues.

Dans le cadre du commerce électronique, si le document original contient un montant à débiter pour valider un achat, un système intermédiaire ne peut pas modifier le montant à débiter car la signature électronique ne
10 correspondrait plus au document original. Toute modification du document original est impossible par un système intermédiaire qui ne connaît pas la clé privée de l'émetteur et a donc peu de chances de pouvoir recréer une nouvelle signature électronique valide.

Une duplication du document original et de sa signature pourrait
15 permettre au système intermédiaire de transmettre à nouveau le document original avec une signature valide au récepteur de façon par exemple à débiter plusieurs fois le compte de l'émetteur. Divers moyens permettent d'éviter cet inconvénient tels que par exemple l'insertion d'une date dans le document original.

20 L'intérêt de la signature électronique qui ressort des explications précédentes ne se limite pas au commerce électronique. Les domaines d'application sont nombreux et variés. La signature électronique peut servir par exemple à authentifier un accord donné sur un contrat, des références de dossier médical, etc.

25 Cependant de nombreux problèmes restent posés pour augmenter la confiance accordée à une signature électronique, tant pour une personne émettrice que pour une personne réceptrice.

Pour une personne émettrice utilisant un système ouvert tel qu'un ordinateur personnel, une incursion par une personne malveillante dans
30 l'ordinateur peut y placer des composants qui détournent les actions de la personne émettrice sur l'ordinateur personnel. Une incursion physique est possible en absence de la personne émettrice, une incursion logique par le réseau est possible même en présence de la personne émettrice, l'aptitude des

virus informatiques à modifier le comportement de programmes est par exemple bien connue. Les visées de telles incursions sont nombreuses, accéder à la valeur de la clé privée, remplacer la valeur de la clé privée par une valeur connue, remplacer le document original par un autre document avant le

5 moment où le document original est appelé à être haché ou chiffré.

Les motifs légitimes d'inquiétude de la personne émettrice se répercutent à la personne réceptrice. Même si la personne réceptrice reçoit une signature valide, la personne émettrice peut vouloir répudier cette signature en prétextant qu'elle a été faite à son insu.

10 Une détention secrète de la clé privée par la personne émettrice elle-même est de fiabilité discutable. La personne émettrice peut vouloir prétendre que la valeur de clé secrète lui a été soustraite dans un moment d'égarement ou plus simplement au moment de sa communication au système cryptographique.

15 Pour pallier les inconvénients qui ressortent de l'état actuel de la technique, l'invention a pour objet un appareil pour effectuer des transactions comprenant un boîtier ayant une protection contre les effractions auquel sont intégrés:

- 20 - un circuit d'interface pour recevoir un support d'identification comportant un circuit logique d'identification;
- des moyens d'interface homme-machine pour présenter des données transactionnelles à un utilisateur et recueillir de l'utilisateur des données d'identification transmises au circuit logique du support via le circuit d'interface ainsi que des commandes de signature en
- 25 relation avec les données transactionnelles présentées;
- un circuit protégé pour délivrer une première signature des données transactionnelles présentées en réponse aux commandes de signature lorsque l'identification a été effectuée, ladite signature étant obtenue en chiffrant une partie au moins des données
- 30 transactionnelles au moyen d'une clé privée de signature stockée de façon non effaçable dans ledit circuit protégé.

Un autre objet de l'invention est un procédé de fabrication d'un appareil pour effectuer des transactions. Le procédé de fabrication comprend une étape de gravure pendant laquelle est généré secrètement un couple de clés cryptographiques duales, constitué d'une clé publique et d'une clé privée de l'appareil, la clé privée étant immédiatement gravée dans un circuit protégé de façon à ne pouvoir laisser aucune trace en dehors dudit circuit protégé, une étape de montage pendant laquelle une interface homme-machine est montée sur un boîtier, le circuit protégé et un circuit d'interface sont montés dans ledit boîtier et pendant laquelle le dit boîtier est fermé de façon à ne plus pouvoir être ouvert ou pénétré sans laisser de trace visible d'effraction.

Un autre objet de l'invention est un procédé pour effectuer des transactions au moyen d'un appareil constitué d'un boîtier qui laisse une trace visible de toute tentative d'effraction, ledit boîtier comprenant des moyens d'interface homme-machine et un circuit d'interface avec un objet physique d'identification. Le procédé comprend une étape de présentation pendant laquelle au moins une donnée transactionnelle est communiquée à l'appareil qui l'affiche sur les moyens d'interface homme-machine, une étape d'identification pendant laquelle un support d'identification comportant un circuit logique d'identification est mis en contact avec le circuit d'interface et des premières données d'identification sont recueillies de l'utilisateur par les moyens d'interface homme-machine puis transmises au circuit logique d'identification qui délivre un signal d'identification s'il reconnaît les dites données d'identification, une étape de signature pendant laquelle, une commande de signature recueillie sur les moyens d'interface homme-machine est transmise dans le boîtier à un circuit protégé qui, si les dites données d'identification sont reconnues par le circuit d'identification, signe une partie au moins des données transactionnelles au moyen d'une clé privée de signature stockée de façon non effaçable dans ledit circuit protégé.

D'autres détails et avantages ressortent de la description d'un mode de mise en œuvre de l'invention, telle qu'elle suit en référence aux figures où :

- la figure 1 présente un appareil conforme à l'invention ;
- la figure 2 présente un procédé de fabrication conforme à l'invention ;

- la figure 3 présente un environnement possible de mise en œuvre de l'invention ;

- la figure 4 présente un procédé d'utilisation conforme à l'invention;

- la figure 5 présente un circuit protégé conforme à l'invention.

5 La figure 1 présente en vue schématique éclatée, un appareil 1, objet de l'invention. Cet appareil comporte un boîtier protégé contre les effractions. Cette protection peut être de différents niveaux:

- 10 - le boîtier peut présenter des traces visibles, par exemple cassure de la coque, dès qu'il se produit une tentative d'effraction (niveau "tamper evident");
- le boîtier peut avoir une structure robuste de façon à résister aux tentatives d'effraction (niveau "tamper resistant");
- 15 - le boîtier peut détecter toute tentative d'effraction pour détruire ou endommager gravement des composants de l'appareil (niveau "tamper responsive").

Dans l'illustration, le boîtier se compose de deux demi boîtiers 13 et 14. En sortie de fabrication, le demi-boîtier inférieur 13 et le demi boîtier supérieur 14 forment un boîtier unique tel que toute tentative d'effraction ou toute effraction laisse une trace visible, cassure ou destruction.

20 L'appareil 1 comprend une ouverture 2 dans laquelle il est possible d'introduire un support d'identification 18. Le support d'identification 18 a pour fonction celle d'une clé physique d'utilisation de l'appareil. Le support d'identification 18 comprend un circuit logique d'identification 40 de manière connue par exemple lorsque le support d'identification est une carte à puce.

25 Une introduction du support d'identification dans l'ouverture 2 se fait jusqu'à mettre le circuit d'identification 40 en contact avec un circuit d'interface 10 relié à un bus système 11 interne à l'appareil 1.

30 Un circuit électrique logique 9 est relié au bus système 11 pour exécuter une ou des séquences de dialogue avec l'objet physique d'identification. De façon avantageuse, les séquences de dialogue font partie de programmes stockés dans une mémoire à accès aléatoire 5 reliée au bus système 11. Le circuit électrique logique 9 est alors un microprocesseur qui exécute des

instructions de programme au moyen d'un système d'exploitation stocké lui aussi dans la mémoire à accès aléatoire 5.

Une interface opérateur sur le boîtier de l'appareil 1, comprend un clavier à touches 3 et un écran 4. Le clavier à touches 3 et l'écran 4 sont
5 fixement reliés dans l'appareil 1, à un circuit d'entrée-sortie 8. Le circuit d'entrée-sortie 8 relié au bus système 11, permet au circuit logique 9 d'exécuter une ou des séquences de dialogue avec l'interface opérateur au moyen des programmes stockés dans la mémoire à accès aléatoire 5.

Un circuit de communication 7 relié à l'intérieur du boîtier au bus
10 système 11 et à l'extérieur du boîtier à un connecteur 12, permet au circuit logique 9 d'exécuter une ou des séquences de communication au moyen des programmes stockés dans la mémoire à accès aléatoire 5. Le connecteur 12 est prévu pour être relié à un ordinateur, un réseau câblé, un modem ou un réseau aérien. Suivant le mode de raccordement choisi, le connecteur 12 est
15 un connecteur à broches, un émetteur récepteur infrarouge ou une antenne.

L'appareil 1 comprend encore un circuit protégé 6. Le circuit 6 est par exemple de type circuit intégré, protégé par une enveloppe robuste qui résiste aux tentatives d'effraction (niveau "tamper resistant") ou dont toute tentative d'effraction endommage le circuit 6 (niveau "tamper responsive").

20 En référence à la figure 5, le circuit protégé 6 comprend une partie dialogue 18 et une partie mémoire 36 à accès en lecture seule. La partie dialogue 18 est prévue pour échanger des informations avec le bus 11. La partie mémoire 36 est de type non effaçable telle que par exemple une mémoire ROM. La partie mémoire 36 contient des données qui y ont été
25 inscrites lors de la fabrication de l'appareil 1.

En particulier, la partie mémoire 36 contient une clé logique privée SK-DEV. Le circuit protégé 6 comprend aussi une partie de traitement arithmétique et logique 39 pour exécuter au moyen d'un système d'exploitation, des fonctions microprogrammées contenues dans une partie mémoire à accès
30 aléatoire 35 du circuit protégé 6. Parmi les fonctions microprogrammées, on distingue des fonctions de chiffrement de données au moyen de la clé privée SK-DEV et d'algorithmes connus en cryptographie. Parmi les fonctions microprogrammées, on distingue aussi des fonctions d'ordonnancement pour

activer les fonctions de chiffrement en réponse à des commandes reçues par la partie dialogue 31. Le circuit protégé 6 est réalisé de façon à ce que la valeur de la clé logique privée SK-DEV ne peut jamais être transmise à l'extérieur du circuit protégé 6.

- 5 Ainsi, lorsque le circuit protégé 6 reçoit sur sa partie dialogue 31, des données transactionnelles et des commandes pour signer les données transactionnelles, les fonctions d'ordonnancement activent les fonctions de chiffrement à l'intérieur du circuit protégé 6, de façon à chiffrer au moins une partie des données transactionnelles au moyen de la clé privée SK-DEV qui
10 reste confinée dans le circuit protégé 6. La clé privée SK-DEV est alors une clé de signature et la signature obtenue est mise à disposition par le circuit protégé 6 sur sa partie dialogue 31.

- Une variante de réalisation possible du circuit protégé 6 consiste à y intégrer un premier module d'entrée-sortie 32 destiné à être relié directement
15 au circuit d'interface 10, un deuxième module d'entrée-sortie 34 destiné à être relié directement à l'écran 4, un troisième module d'entrée-sortie 33 destiné à être relié directement au clavier 3, un quatrième modules d'entrée-sortie 37 destiné à être relié directement aux moyens de communication tels que le connecteur 12. Les modules 33 et 34 remplacent alors le circuit d'entrée sortie
20 8 dans l'appareil 1. Le module 37 remplace le circuit de communication 7.

- En référence à la figure 2, le procédé de fabrication de l'appareil 1 comprend une étape 15 dans laquelle est créé un couple de clés logiques de chiffrement au moyen d'un générateur de nombres selon des méthodes connues dans le domaine de la cryptographie, de façon à ce que ce couple de
25 clés permette de mettre en œuvre un cryptosystème à clé publique connu tel que par exemple RSA. Une première clé constitue la clé privée SK-DEV qui est gravée dans la partie mémoire 36 du circuit protégé 6 dès la création du couple de clés, et ceci de façon à ce qu'aucune copie de la valeur de la clé privée SK-DEV ne subsiste ailleurs que dans le circuit protégé 6.

- 30 Les opérations du générateur de nombre depuis la création du couple de clés jusqu'à la gravure de la clé privée dans le circuit protégé 6 sont occultées de sorte que le fabricant de l'appareil ne puisse jamais avoir connaissance de la clé privée SK-DEV.

La deuxième clé du couple constitue une clé publique PK-DEV qui elle, n'est pas nécessairement conservée dans la partie mémoire non effaçable 36 mais peut l'être ailleurs en vue de traitements ultérieurs.

5 Toutefois, graver la clé publique PK-DEV dans la partie mémoire non effaçable 36 procure un avantage supplémentaire, celui de s'assurer que la clé publique ne sera jamais perdue tant que le circuit protégé 6 ne sera pas altéré. La conservation de la clé publique sur un autre support, mémoire à accès aléatoire 5 de l'appareil, base de donnée extérieure, inscription visible, est acceptable mais nécessite cependant une gestion adaptée à une conservation
10 sure de la clé publique PK-DEV.

Un autre avantage supplémentaire est procuré en gravant aussi dans la partie mémoire 36 non effaçable du circuit protégé 6, un numéro d'identification de l'appareil 1. Comme une gravure sur une plaque constructeur, le numéro d'identification permet de faire un suivi de l'appareil. La gravure du numéro
15 d'identification dans la partie mémoire non effaçable 36 rend disponible cette donnée pour effectuer des traitements informatiques. Le numéro d'identification est par exemple constitué d'une première série de caractères qui identifie le fabricant de l'appareil et d'une deuxième série de caractères qui identifie l'appareil dans le lot de ceux produits par le fabricant.

20 Dans une étape 16, les composants 7 à 11 sont montés dans le demi boîtier inférieur 13. Le clavier à touche 3 et l'écran 4 sont montés sur le boîtier et sont raccordés au circuit d'entrée sortie 8, le connecteur 12 est raccordé au circuit de communication 7 et le demi boîtier supérieur 14 est fixé sur le demi boîtier inférieur 13 de façon à constituer un boîtier unique qui enferme
25 hermétiquement les composants 5 à 11, et de façon à ce que le boîtier ainsi constitué ne puisse plus être réouvert sans y provoquer une altération irréversible et clairement visible.

Divers méthodes connues sont possibles pour faire que toute ouverture, pénétration, tentative d'ouverture ou de pénétration, laisse une trace visible
30 d'effraction. On peut munir le demi boîtier inférieur 13 et le demi boîtier supérieur 14 de clips à enfichage unique avec cassure au désenfichage. Au lieu de deux demi boîtiers, on peut noyer les divers éléments de l'appareil 1 dans une résine homogène.

Tant le procédé de fabrication que la structure inviolable de l'appareil 1 fait que la valeur de la clé privée SK-DEV n'est connue de personne. La valeur de la clé SK-DEV est inconnue du fabricant car sa création par le générateur aléatoire de nombres et sa gravure dans le circuit protégé 6 ne sont pas
5 accessibles.

La valeur de la clé SK-DEV est inconnue de toute personne ayant l'appareil entre les mains car le système d'exploitation de l'appareil 1 ne permet pas de lecture de la valeur de la clé privée SK-DEV. En particulier, la valeur de la clé privée SK-DEV ne peut pas être communiquée au circuit d'entrée-sortie 8
10 et donc, ne peut jamais apparaître sur l'écran 4. Ainsi, tout utilisateur de l'appareil 1 ne risque pas de divulguer, volontairement ou involontairement, la valeur de la clé privée SK-DEV.

La valeur de la clé privée SK-DEV de l'appareil, est inconnue de toute personne ou de tout système en communication avec l'appareil car cette valeur
15 ne peut pas être recopiée ni dans la mémoire à accès aléatoire 5, ni dans le circuit d'interface 10, ni dans le circuit de communication 7.

La seule solution qui reste à un individu malveillant est celle d'ouvrir le boîtier de l'appareil 1 par exemple pour corrompre le système d'exploitation en remplaçant un ou plusieurs des composants 5 à 11 ou pour tenter d'interférer
20 avec le circuit protégé 6. Cependant la constitution du boîtier fait que cette ouverture laisse nécessairement des traces d'effraction visibles. Devant ces traces d'effraction visibles, le détenteur de l'appareil a conscience que toute utilisation se fait à ses risques et périls et qu'il se doit de signaler cette effraction au même titre qu'il se doit de signaler une perte de l'appareil pour
25 faire opposition définitive à toute utilisation future. De plus, même une ouverture du boîtier ne permet pas de prendre connaissance de la clé privée SK-DEV car celle-ci reste confinée dans le circuit protégé 6.

L'ordre dans lequel sont représentées les étapes 15 et 16 sur la figure 2, est sans importance. L'étape 16 peut précéder l'étape 15 si le circuit protégé 6
30 génère lui-même le couple de clés lorsque celui-ci est déjà monté dans le boîtier.

Une étape de certification 30 permet au fabricant de certifier l'origine de l'appareil (1). Pendant l'étape 30, le fabricant élabore une chaîne de

- caractères comprenant au moins la clé publique PK-DEV de l'appareil ou un numéro d'identification de l'appareil. La chaîne de caractère est chiffrée au moyen d'une clé privée SK-FAB du fabricant, de façon à obtenir une signature de certification. La signature de certification est mémorisée dans l'appareil.
- 5 L'étape 30 peut être mise en œuvre en même temps que l'étape 15. L'étape 30 peut aussi être mise en œuvre après fabrication, par exemple pour certifier à nouveau l'appareil 1 suite à une révision. L'appareil 1 contient alors un programme qui vérifie une concordance de la signature de certification avec certaines données telles que la clé publique PK-DEV de l'appareil ou le numéro
- 10 d'identification de l'appareil, stockées dans le circuit protégé 6, lors d'un chargement de la signature de certification en mémoire 5 ou 35.

La figure 3 montre un environnement possible d'utilisation de l'appareil 1.

- Un individu émetteur 17 consulte par exemple un catalogue d'achats en
- 15 ligne au moyen d'un ordinateur personnel 19 muni d'un écran 20, d'un clavier 21 et d'une souris 22. L'ordinateur 20 est raccordé à un réseau ouvert 23, par exemple l'Internet, auquel sont également raccordés des serveurs 24, 25. Le serveur 25 transmet sur le réseau 23 des pages du catalogue d'achats en ligne. L'individu émetteur 17 sélectionne sur l'écran 20 au moyen de la souris
- 20 22 un article d'une page de catalogue dont le prix est affiché. L'individu émetteur 17 déclenche ensuite une transaction pour commander et payer cet article.

- Cette transaction permet à un organisme vendeur détenteur du serveur 25, de se faire payer par un organisme financier détenteur du serveur 24, de
- 25 façon à livrer l'article sélectionné à l'individu émetteur 17.

- L'individu émetteur 17 veut être sûr que le montant débité de son compte sur le serveur 24 se limite au montant qui correspond au prix d'achat de l'article sélectionné. Le montant débité ne doit donc pas pouvoir être modifié dans le système informatique ouvert qui comprend l'ordinateur
- 30 personnel 19, le réseau ouvert 23, le serveur 24 et/ou le serveur 25. Dans le cadre particulier d'une transaction financière, l'individu émetteur veut de plus être prémuni contre un débit multiple du montant sur lequel il donne une seule fois son accord.

Le serveur 25 doit être assuré que le montant de la transaction est incontestablement débité à son profit par le serveur 24. En particulier, la transaction ne doit pas pouvoir être répudiée de façon incontrôlée.

Le serveur 24 doit être assuré que la transaction est véritablement
5 déclenchée avec l'accord de l'individu émetteur 17.

Pour garantir la confiance des intervenants à la transaction, la transaction met en œuvre un procédé d'authentification du montant à débiter qui marque avec certitude l'accord de l'individu 17. Dans l'exemple de la figure 3, le montant à débiter fait partie de données transactionnelles à signer au
10 moyen du procédé expliqué maintenant en référence à la figure 4.

Pendant une étape de présentation 26, la donnée transactionnelle à signer, est communiquée à l'appareil 1 précédemment décrit. L'appareil 1 affiche alors la donnée transactionnelle à signer, sur l'écran 4.

Lorsque dans l'exemple de la figure 3, l'individu 17 tient entre ses mains
15 l'appareil 1, il a de bonnes raisons de faire confiance au montant affiché sur l'écran 4 car il peut contrôler que le boîtier n'a aucune trace visible d'effraction et donc que ce montant est bien celui effectivement traité par l'appareil 1.

L'individu émetteur 17 peut par exemple en mode itinérant, communiquer lui-même le montant de la transaction à l'appareil 1 en utilisant le
20 clavier 3. Faire communiquer le montant de la transaction à l'appareil 1 par le système informatique offre l'avantage d'une plus grande simplicité lorsque l'appareil 1 dispose d'une liaison de communication avec l'ordinateur personnel 19 sur la figure 3, au moyen du connecteur 12.

Pendant une étape d'identification 27, un support d'identification 18 est
25 mis en contact avec le circuit d'interface 10. Un code est tapé sur le clavier 3 pour identifier la personne qui effectue la transaction.

Dans l'exemple de la figure 3, l'objet physique d'identification est typiquement une carte de crédit que l'individu 17 introduit dans l'ouverture 2 jusqu'à mise en contact avec le circuit d'interface 10. Le code tapé est
30 typiquement son code confidentiel à quatre chiffres suivi d'une validation. L'individu 17 se fait ainsi reconnaître par l'appareil 1.

Le circuit logique 9 exécute une séquence d'instructions stockée en mémoire 5 pour transmettre à l'objet d'identification 18, la valeur du code tapé

sur le clavier 3. Dans le cas où le circuit protégé 6 est directement raccordé au clavier 3 et au circuit d'interface 10, le circuit protégé 6 exécute une séquence d'instructions stockée en mémoire 35 pour transmettre à l'objet d'identification 18, la valeur du code tapé sur le clavier 3. Si le code correspondant est
5 reconnu par le support d'identification, celui-ci émet un signal d'identification sur le circuit d'interface 10 à destination du circuit protégé 6, effectuant ainsi une identification de l'individu qui a tapé le code. Dans l'interface homme-machine, le clavier 3 peut être remplacé par des moyens de reconnaissance bio métrique; dans ce cas, une donnée bio métrique de l'individu 17 est
10 substituée au code précédemment mentionné.

Pendant une étape de signature 28, l'individu 17 tape une commande de signature sur le clavier 3. La commande de signature est transmise au circuit protégé 6 dans le boîtier. A réception de la commande de signature, s'il a reçu le signal d'identification, le circuit protégé 6 exécute une opération de
15 chiffrement qui porte sur la donnée transactionnelle affichée sur l'écran 4. L'opération de chiffrement accède à la clé privée de signature SK-DEV confinée dans la partie mémoire non effaçable 36 du circuit protégé 6 à l'intérieur du boîtier, signant ainsi avec certitude la donnée affichée sur l'écran 4.

20 Lorsqu'on souhaite signer la donnée affichée sur l'écran 4, corrélativement à une autre donnée transactionnelle, les données sont concaténées par le circuit logique 9 ou directement par le circuit protégé 6 avant l'opération de chiffrement.

L'autre donnée transactionnelle concerne par exemple les références
25 d'un compte à débiter. Ces références sont dans l'exemple de la figure 3, procurées par l'objet physique d'identification 18 qui est une carte de crédit.

Pendant l'étape de signature 28, il est avantageux d'appliquer une fonction de hachage à sens unique avant l'opération de chiffrement. La fonction de hachage permet de réduire la taille d'une chaîne de données à chiffrer et
30 d'accélérer ainsi l'opération de chiffrement au moyen de la clé privée et une opération de déchiffrement au moyen de la clé publique. Le fait pour la fonction de hachage d'être à sens unique rend difficile à un tiers de créer une autre chaîne de données telle que l'application de la fonction de hachage à cette

autre chaîne de données donne le même résultat que la fonction de hachage appliquée à la chaîne de données originale.

Dans l'exemple de la figure 3, il est intéressant d'ajouter une étape de communication 29. Pendant l'étape de communication 29, le résultat du
5 chiffrement est émis sous forme de message à destination du système informatique au moyen du connecteur 12 en liaison avec l'ordinateur 19.

L'étape d'identification 27 peut précéder l'étape de présentation 26, par exemple pour permettre à l'individu 17 de se faire identifier en vue de plusieurs transactions successives pour chacune desquelles l'étape de présentation 27
10 et l'étape de signature 28 sont alors répétées.

Ainsi les étapes 26 à 28 assurent à l'individu 17 que l'appareil 1 a signé le montant affiché sur l'écran 4, en le concaténant pour le cas particulier d'une transaction financière au numéro de compte à débiter. En déchiffrant le message émis en étape 29, au moyen de la clé publique correspondant à la clé
15 privée de l'appareil 1, le serveur 24 est assuré que le message a bien été émis par l'appareil 1 sans avoir pu être corrompu par le système informatique car la clé privée de signature est confinée dans le circuit protégé 6 à l'intérieur de l'appareil 1. Le serveur 24 peut alors débiter le compte référencé dans le message du montant transmis dans le message car l'appareil 1 authentifie
20 qu'un accord a été donné au moyen de la carte de crédit 18 et de son code confidentiel. Le serveur 25 a de bonnes raisons de croire que la transaction entre l'individu 17 et le serveur 24 ne sera pas répudiée car celle-ci s'est faite dans un mode hautement sécuritaire.

On peut concevoir que le serveur 24 prend connaissance de la clé
25 publique de l'appareil 1 en consultant une base de donnée qui répertorie tous les appareils 1 dignes de confiance. La tenue à jour de cette base de donnée nécessite alors un minimum de gestion. Il est plus simple et plus rapide que l'appareil 1 transmette lui-même sa clé publique pendant l'étape 29. Ceci présente un danger si un élément du système informatique tente de simuler
30 l'appareil 1 en créant un couple de clés privées et publiques.

Pour éviter le danger précédemment mentionné, l'appareil 1 émet à destination du système informatique, une chaîne de caractères comprenant une valeur de clé publique duale de sa clé privée de signature, en émettant

simultanément une deuxième signature dite signature de certification. Pour assurer que l'appareil 1 est un appareil légitime, le fabricant applique une fonction de hachage à sens unique à la chaîne de caractères et chiffre le résultat de la fonction de hachage au moyen d'une clé privée SK-FAB du fabricant. Le résultat du chiffrement constitue alors la signature de certification que le fabricant stocke avec la chaîne de caractères dans l'appareil 1. Le serveur 24 n'a alors besoin de connaître que la clé publique du fabricant PK-FAB, commune à de nombreux appareils 1. En effet, lorsque l'appareil 1 transmet la chaîne de caractères contenant la clé publique PK-DEV de l'appareil en clair, avec la signature de certification au système informatique, il suffit au serveur 24 d'appliquer la fonction de hachage à sens unique à la chaîne de caractère contenant la clé publique PK-DEV de l'appareil 1 et à déchiffrer la signature de certification au moyen de la clé publique PK-FAB du fabricant. Si le résultat de la fonction de hachage est identique au résultat du déchiffrement, le serveur 24 est assuré que la clé publique de l'appareil 1 est une clé publique légitime et donc que l'appareil 1 a été utilisé de façon certaine pour signer tout ou partie des données transactionnelles.

REVENDICATIONS

1. Appareil (1) pour effectuer des transactions comprenant un boîtier
5 ayant une protection contre les effractions auquel sont intégrés:
- un circuit d'interface (10) pour recevoir un support d'identification comportant un circuit logique d'identification;
 - des moyens d'interface homme-machine (3,4) pour
10 présenter des données transactionnelles à un utilisateur et recueillir de l'utilisateur des données d'identification transmises au circuit logique du support via le circuit d'interface (10) ainsi que des commandes de signature en relation avec les données transactionnelles présentées;
 - un circuit protégé (6) pour délivrer une première signature
15 des données transactionnelles présentées en réponse aux commandes de signature lorsque l'identification a été effectuée, ladite signature étant obtenue en chiffrant une partie au moins des données transactionnelles au moyen d'une clé privée de signature stockée de façon non effaçable dans ledit circuit protégé.
- 20 2. Appareil (1) pour effectuer des transactions selon la revendication 1, caractérisé en ce qu'il comprend un moyen de communication (12) pour échanger des données avec un système informatique.
3. Appareil (1) pour effectuer des transactions selon l'une des
25 revendications précédentes, caractérisé en ce que le circuit protégé (6) contient une clé publique duale de ladite clé privée, stockée de façon non effaçable.
4. Appareil (1) pour effectuer des transactions selon l'une des
30 revendications précédentes, caractérisé en ce que le circuit protégé (6) contient un numéro d'identification de l'appareil, stocké de façon non effaçable.

5. Appareil (1) pour effectuer des transactions selon l'une des revendications précédentes, caractérisé en ce qu'une mémoire (5, 35) contient une signature certifiant une origine de l'appareil (1).

5 6. Procédé de fabrication d'un appareil (1) pour effectuer des transactions, caractérisé en ce qu'il comprend:

- une étape de gravure (15) pendant laquelle est généré secrètement un couple de clés cryptographiques duales, constitué d'une clé publique et d'une clé privée de l'appareil, la clé privée étant
10 immédiatement gravée dans un circuit protégé (6) de façon à ne pouvoir laisser aucune trace en dehors dudit circuit protégé (6);
- une étape de montage (16) pendant laquelle une interface homme-machine (3,4) est montée sur un boîtier, le circuit protégé(6) et un circuit d'interface (10) sont montés dans ledit boîtier et pendant
15 laquelle le dit boîtier est fermé de façon à ne plus pouvoir être ouvert ou pénétré sans laisser de trace visible d'effraction.

7. Procédé de fabrication d'un appareil (1) pour effectuer des transactions selon la revendication 6, caractérisé en ce que pendant l'étape de
20 gravure (15), la clé publique est gravée dans le circuit protégé (6).

8. Procédé de fabrication d'un appareil (1) pour effectuer des transactions selon la revendication 6 ou 7, caractérisé en ce que pendant l'étape de gravure (15), un numéro d'identification de l'appareil (1) est gravé
25 dans le circuit protégé (6).

9. Procédé de fabrication d'un appareil (1) pour effectuer des transactions selon l'une des revendications précédentes, caractérisé en ce qu'il comprend une étape de certification pendant laquelle une chaîne de caractères
30 comprenant au moins la clé publique ou le numéro d'identification, est chiffrée au moyen d'une clé fabriquant privée, de façon à obtenir une signature certifiant l'origine de l'appareil (1) et en ce que cette signature est mémorisée dans l'appareil.

10. Procédé pour effectuer des transactions au moyen d'un appareil (1) constitué d'un boîtier qui laisse une trace visible de toute tentative d'effraction, ledit boîtier comprenant des moyens d'interface homme-machine (3,4) et un circuit d'interface (10) avec un objet physique d'identification, caractérisé en ce qu'il comprend:

- une étape de présentation pendant laquelle au moins une donnée transactionnelle est communiquée à l'appareil (1) qui l'affiche sur les moyens d'interface homme-machine (3,4);
- 10 - une étape d'identification pendant laquelle un support d'identification comportant un circuit logique d'identification est mis en contact avec le circuit d'interface (10) et des premières données d'identification sont recueillies de l'utilisateur par les moyens d'interface homme-machine (3,4) puis transmises au circuit logique d'identification
- 15 qui délivre un signal d'identification s'il reconnaît les dites données d'identification;
- une étape de signature pendant laquelle, une commande de signature recueillie sur les moyens d'interface homme-machine (3,4) est transmise dans le boîtier à un circuit protégé (6) qui, si les dites
- 20 données d'identification sont reconnues par le circuit d'identification, signe une partie au moins des données transactionnelles au moyen d'une clé privée de signature stockée de façon non effaçable dans ledit circuit protégé (6).

25 11. Procédé pour effectuer des transactions au moyen d'un appareil (1) selon la revendication 10, caractérisé en ce que pendant l'étape de signature, ladite partie au moins des données transactionnelles, est concaténée à une deuxième donnée d'identification procurée par le circuit d'identification de façon à ce que la signature au moyen de la clé privée de

30 signature porte sur le résultat de la concaténation.

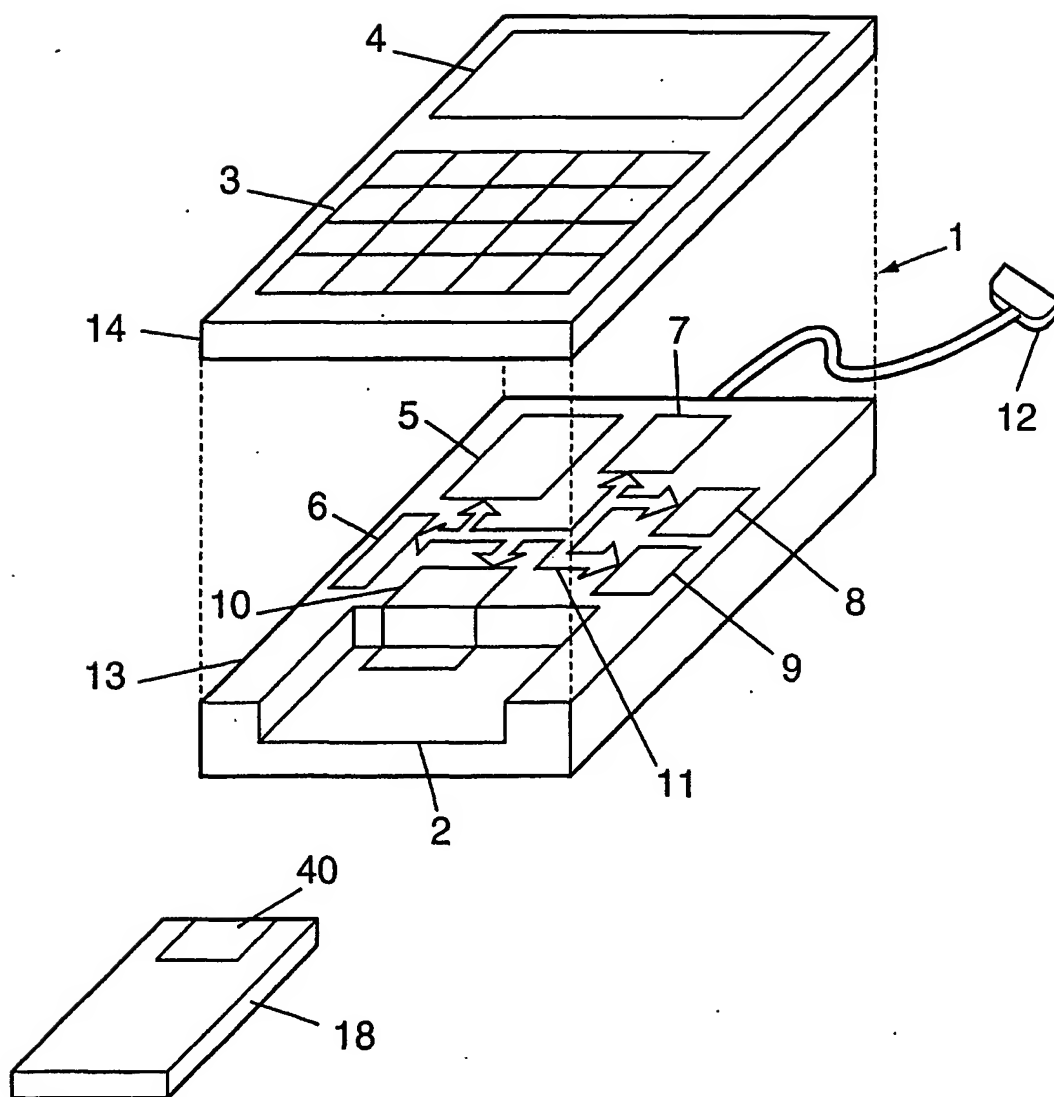
12. Procédé pour effectuer des transactions au moyen d'un appareil (1) selon l'une des revendications 10 ou 11, caractérisé en ce qu'il comprend une étape de communication pendant laquelle la signature est émise par l'appareil (1) à destination d'un système informatique.

5

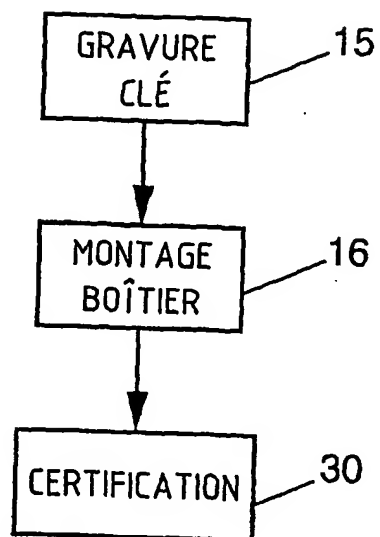
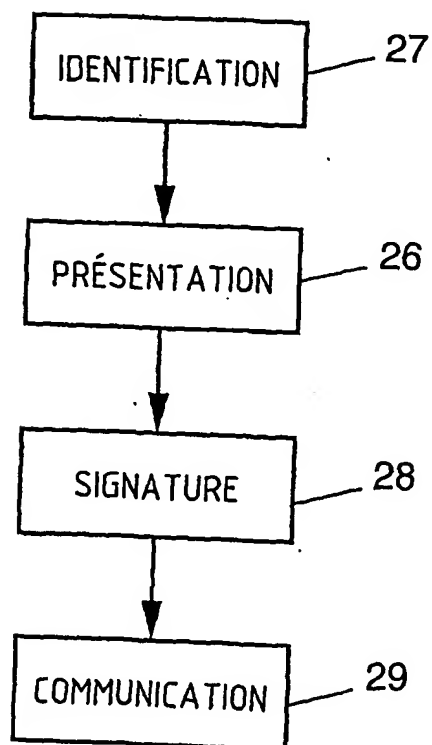
13. Procédé pour effectuer des transactions au moyen d'un appareil (1) selon la revendication 12, caractérisé en ce que pendant l'étape de communication, l'appareil (1) émet à destination du système informatique, une chaîne de caractères comprenant au moins une valeur de clé publique duale
10 de la clé privée de signature, accompagnée d'une signature de certification de ladite chaîne de caractères.

1/4

FIG. 1

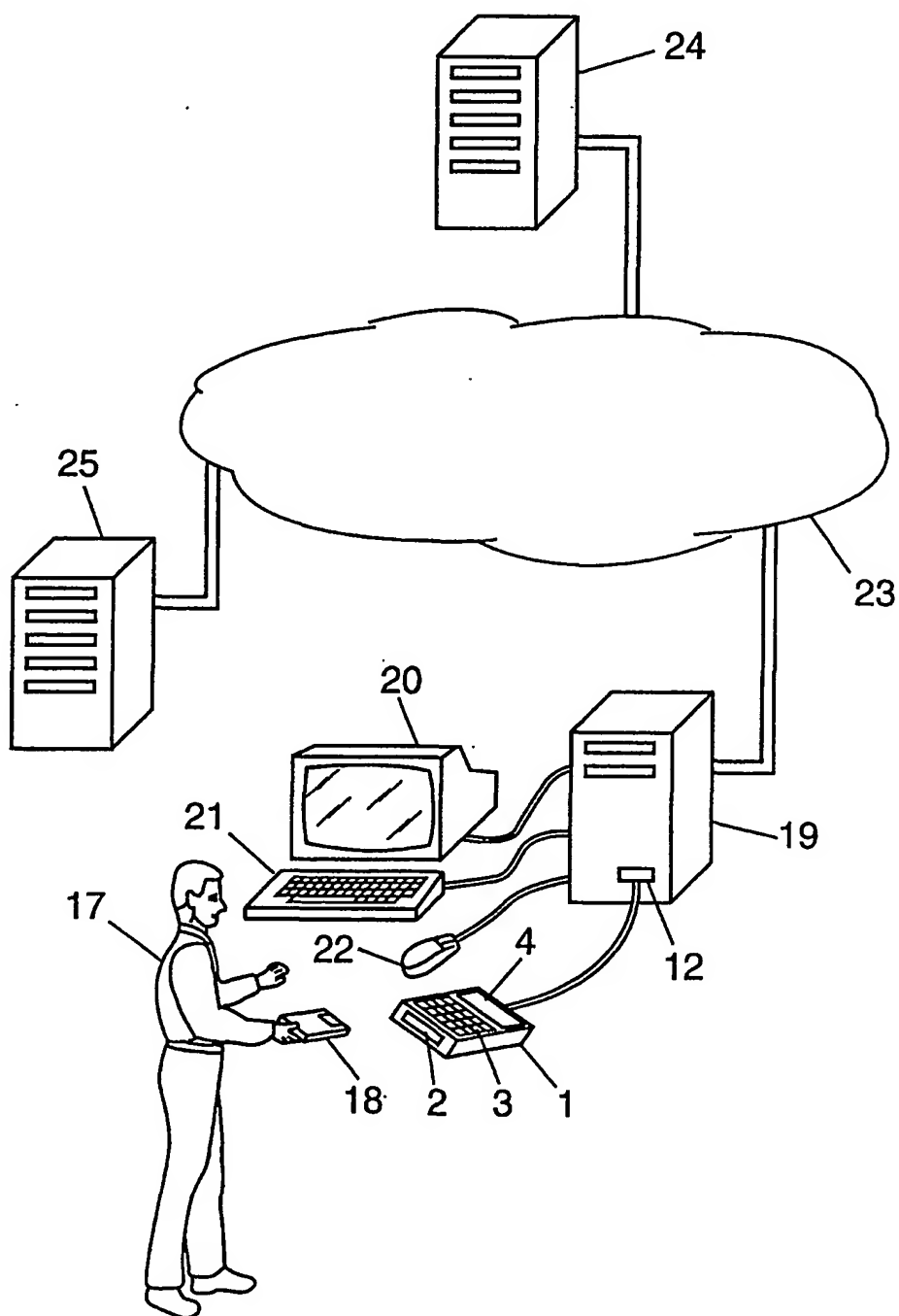


2/4

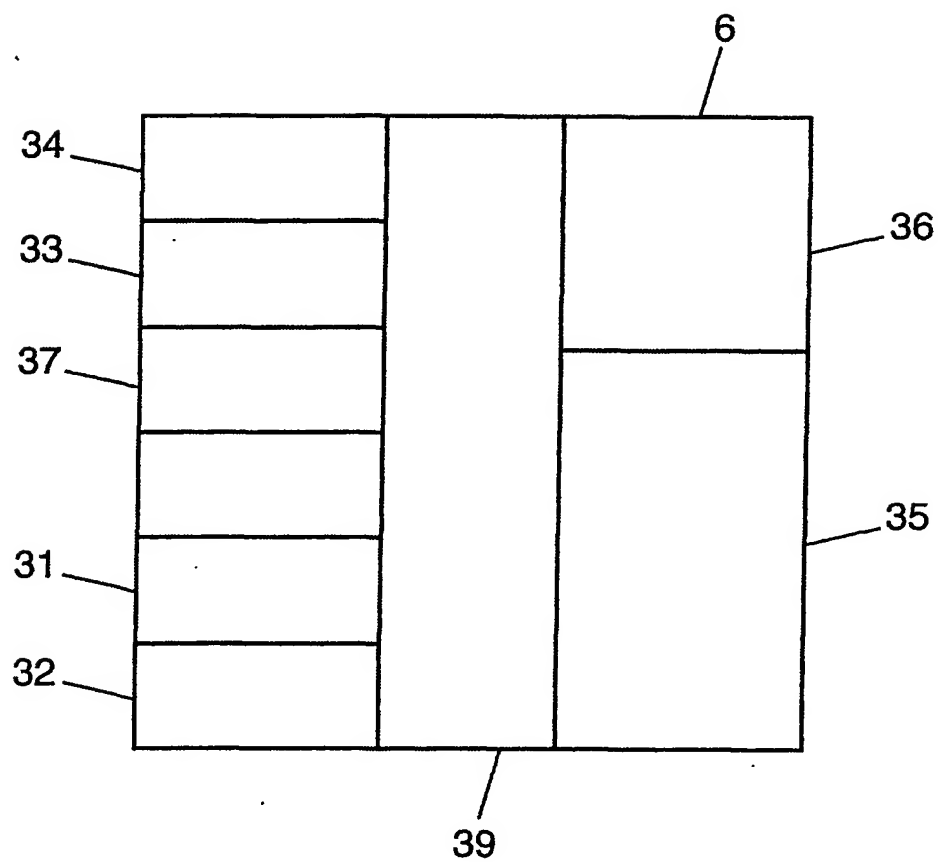
FIG. 2**FIG. 4**

3/4

FIG. 3



4/4

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 01/03569

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 731 842 A (SMITH PETER R) 15 March 1988 (1988-03-15) abstract the whole document	1,2,4-6, 8-12
X	WO 00 26838 A (SMARTDISK CORP) 11 May 2000 (2000-05-11)	10-12
A	page 27, line 14 -page 30, line 11 claims 14-19	1-9,13
A	FR 2 779 018 A (ACTIVCARD) 26 November 1999 (1999-11-26) abstract page 39, line 7 -page 40, line 16 figure 9	1-13
	— -/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the International filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the International filing date but later than the priority date claimed

- *T* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *Z* document member of the same patent family

Date of the actual completion of the International search

15 April 2002

Date of mailing of the International search report

22/04/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van Dop, E

INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 01/03569

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 098 053 A (SLATER ALAN) 1 August 2000 (2000-08-01) column 4, line 31 -column 5, line 25 column 7, line 66 -column 9, line 12 figures 1-3	1-13
A	US 5 517 569 A (CLARK DERECK B) 14 May 1996 (1996-05-14) abstract column 2, line 19 - line 67 figure 2	1-13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 01/03569

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 4731842	A	15-03-1988	GB 2168514 A DE 3585439 D1 EP 0186981 A2 JP 61139878 A	18-06-1986 02-04-1992 09-07-1986 27-06-1986
WO 0026838	A	11-05-2000	AU 1602500 A WO 0026838 A1	22-05-2000 11-05-2000
FR 2779018	A	26-11-1999	FR 2779018 A1 AT 213857 T AU 3830399 A CA 2330534 A1 DE 69900934 D1 EP 1004101 A1 WO 9962037 A1 TW 405105 B	26-11-1999 15-03-2002 13-12-1999 02-12-1999 04-04-2002 31-05-2000 02-12-1999 11-09-2000
US 6098053	A	01-08-2000	AU 5587999 A EP 0982674 A2 WO 0022559 A1 GB 2333878 A , B	01-05-2000 01-03-2000 20-04-2000 04-08-1999
US 5517569	A	14-05-1996	AU 691602 B2 AU 2190295 A BR 9507114 A CA 2185697 A1 EP 0750812 A1 JP 10500504 T NZ 283566 A WO 9526085 A1 US 5815577 A	21-05-1998 09-10-1995 02-09-1997 28-09-1995 02-01-1997 13-01-1998 19-12-1997 28-09-1995 29-09-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 01/03569

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 4 731 842 A (SMITH PETER R) 15 mars 1988 (1988-03-15) abrégé le document en entier	1,2,4-6, 8-12
X	WO 00 26838 A (SMARTDISK CORP) 11 mai 2000 (2000-05-11)	10-12
A	page 27, ligne 14 -page 30, ligne 11 revendications 14-19	1-9,13
A	FR 2 779 018 A (ACTIVCARD) 26 novembre 1999 (1999-11-26) abrégé page 39, ligne 7 -page 40, ligne 16 figure 9	1-13
	-/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

T document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 avril 2002

Date d'expédition du présent rapport de recherche internationale

22/04/2002

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tél. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Van Dop, E

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 01/03569

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>US 6 098 053 A (SLATER ALAN) 1 août 2000 (2000-08-01) colonne 4, ligne 31 - colonne 5, ligne 25 colonne 7, ligne 66 - colonne 9, ligne 12 figures 1-3</p> <p>---</p>	1-13
A	<p>US 5 517 569 A (CLARK DERECK B) 14 mai 1996 (1996-05-14) abrégé colonne 2, ligne 19 - ligne 67 figure 2</p> <p>-----</p>	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs

aux familles de brevets

Internationale No

PCT/FR 01/03569

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4731842	A	15-03-1988	GB 2168514 A DE 3585439 D1 EP 0186981 A2 JP 61139878 A	18-06-1986 02-04-1992 09-07-1986 27-06-1986
WO 0026838	A	11-05-2000	AU 1602500 A WO 0026838 A1	22-05-2000 11-05-2000
FR 2779018	A	26-11-1999	FR 2779018 A1 AT 213857 T AU 3830399 A CA 2330534 A1 DE 69900934 D1 EP 1004101 A1 WO 9962037 A1 TW 405105 B	26-11-1999 15-03-2002 13-12-1999 02-12-1999 04-04-2002 31-05-2000 02-12-1999 11-09-2000
US 6098053	A	01-08-2000	AU 5587999 A EP 0982674 A2 WO 0022559 A1 GB 2333878 A , B	01-05-2000 01-03-2000 20-04-2000 04-08-1999
US 5517569	A	14-05-1996	AU 691602 B2 AU 2190295 A BR 9507114 A CA 2185697 A1 EP 0750812 A1 JP 10500504 T NZ 283566 A WO 9526085 A1 US 5815577 A	21-05-1998 09-10-1995 02-09-1997 28-09-1995 02-01-1997 13-01-1998 19-12-1997 28-09-1995 29-09-1998